

Nr referencyjny: RSID.271.39.2025

Załącznik nr 7 do SWZ

Szczegółowy opis przedmiotu zamówienia

Mając na uwadze nadrzędność celu jakim jest skuteczne uruchomienie planowanych rozwiązań Zamawiający zastrzega, że zadaniem Wykonawcy jest dostarczenie wszelkich niezbędnych elementów sprzętowych, oprogramowania, licencji oraz wykonanie wszystkich niezbędnych prac instalacyjnych, konfiguracyjnych i wdrożeniowych, które konieczne są do prawidłowego działania zgodnie z przeznaczeniem, nawet jeśli nie zostały one wymienione w dalszej części niniejszego dokumentu.

Wymagania ogólne

W ramach przedmiotowego zamówienia, Zamawiający wymaga dostarczenia, instalacji oraz konfiguracji sprzętu i oprogramowania, którego parametry minimalne wskazane zostały poniżej. Zamawiający akceptuje sprzęt oraz oprogramowanie o wyższych (lepszych) parametrach użytkowych lub wykonany w nowszej technologii pod warunkiem, że produkty zaoferowane przez Wykonawcę spełniają wszystkie parametry minimalne.

Wszystkie oferowane produkty mają pochodzić z oficjalnego kanału dystrybucyjnego producenta, posiadać wszystkie wymagane certyfikaty i oznaczenia oraz spełniać wszystkie wymagane prawem normy.

Zamawiający wymaga, by dostarczone urządzenia były nowe (tzn. wyprodukowane nie wcześniej, niż na 12 miesięcy przed ich dostarczeniem) oraz by były nieużywane .

Zamawiający wymaga kompleksowego uruchomienia i zainstalowania dostarczonego sprzętu, oprogramowania oraz migracji istniejącego środowiska do dostarczonej platformy.

Ogólne zasady równoważności rozwiązań

W celu zachowania zasad neutralności technologicznej i konkurencyjności dopuszcza się rozwiązania równoważne do wyspecyfikowanych, przy czym za rozwiązanie równoważne uważa się takie rozwiązanie, które pod względem technologii, wydajności i funkcjonalności nie odbiega znacząco od technologii funkcjonalności i wydajności wyszczególnionych w rozwiązaniu wyspecyfikowanym, przy czym nie podlegają porównaniu cechy rozwiązania właściwe wyłącznie dla rozwiązania wyspecyfikowanego, takie jak: zastrzeżone patenty, własnościowe rozwiązania technologiczne, własnościowe protokoły itp., a jedynie te, które stanowią o istocie całości zakładanych rozwiązań technologicznych i posiadają odniesienie w rozwiązaniu równoważnym. W związku z tym, Wykonawca może zaproponować rozwiązania, które realizują takie same funkcjonalności wyspecyfikowane przez Zamawiającego w inny, niż podany sposób, za rozwiązanie równoważne nie można uznać rozwiązania identycznego (tożsamego), a jedynie takie, które w porównywanych cechach wykazuje dokładnie tę samą lub bardzo zbliżoną wartość użytkową. Przez bardzo zbliżoną wartość użytkową rozumie się podobne, z dopuszczeniem nieznacznych różnic niewpływających w żadnym stopniu na całokształt systemu, zachowanie oraz realizowanie podobnych funkcjonalności w danych warunkach, dla których to warunków rozwiązania te są dedykowane. Rozwiązanie równoważne musi zawierać dokumentację potwierdzającą, że spełnia wymagania funkcjonalne Zamawiającego, w tym wyniki porównań, testów,

Nr referencyjny: RSID.271.39.2025

czy możliwości oferowanych przez to rozwiązanie w odniesieniu do rozwiązania wyspecyfikowanego. Dostarczenie przez Wykonawcę rozwiązania równoważnego musi być zrealizowane w taki sposób, aby wymiana oprogramowania na równoważne nie zakłóciła bieżącej pracy Urzędu. W tym celu Wykonawca musi do oprogramowania równoważnego przenieść wszystkie dane niezbędne do prawidłowego działania nowych systemów, przeszkolić użytkowników, skonfigurować oprogramowanie, uwzględnić niezbędną asystę pracowników Wykonawcy w operacji uruchamiania oprogramowania w środowisku produkcyjnym itp.

Wykonawca odpowiedzialny jest za dostawę w pełni funkcjonujących rozwiązań opisanych w niniejszym załączniku, w tym jeżeli jest konieczne, pozyskanie niezbędnych informacji do realizacji zamówienia, zawarcie koniecznych umów itp.

1. Oprogramowanie

Dostarczone systemy oraz wszystkie niezbędne oprogramowanie dodatkowe na serwerach ma być kompletnie zainstalowane, spersonalizowane oraz aktywowane o ile jest to wymagane.

Konfiguracja logiczna sprzętu (nazwy sieciowe, adresy IP, nazwy i konta użytkowników) ma być przeprowadzona zgodnie z zaleceniami Zamawiającego.

2. Sprzęt

Wszystkie dostarczane urządzenia muszą zostać zainstalowane [tj. wypakowane, zmontowane, zamontowane w szafach RACK, uruchomione i skonfigurowane] w docelowym miejscu pracy [wskazanym przez Zamawiającego] w terminie uzgodnionym z Zamawiającym. Wszystkie opakowania zostaną zutylizowane przez i na koszt Wykonawcy.

Zamawiający wydzieli pomieszczenie pod instalację infrastruktury, Wykonawca zainstaluje sprzęt w pomieszczeniu zgodnie z zaleceniami producenta dot. warunków pracy dla dochowania warunków gwarancji pod względem parametrów fizycznych otoczenia i zadba o spełnienie warunków fizycznych dla bezpieczeństwa instalowanej infrastruktury min. w okresie udzielonej gwarancji.

2.1. Serwery

Na serwerach należy zainstalować lub uaktualnić system wirtualizacji i skonfigurować go do korzystania z zasobów dyskowych macierzy. Wykonawca zaprojektuje schemat rozmieszczeń, ilości i przydział zasobów dla wszystkich serwerów wirtualnych wymaganych do realizacji Przedmiotu Zamówienia.

3. Inne wymagania

Oferowane przez Wykonawcę w dniu składania ofert rozwiązania, nie mogą być przeznaczone przez ich producenta do wycofania z produkcji, sprzedaży lub z wsparcia technicznego. Oferowane urządzenia muszą być przypisane w serwisie producenta do Zamawiającego.

Zamawiający wymaga, aby dostarczone oprogramowanie było oprogramowaniem w wersji aktualnej na dzień składania ofert.

Nr referencyjny: RSID.271.39.2025

W celu potwierdzenie spełnienia przez oferowany sprzęt wskazanych w niniejszym dokumencie wymagań, Wykonawca na wezwanie Zamawiającego przedłoży szczegółowy wykaz oferowanego sprzętu, użyte do realizacji zamówienia komponenty, karty katalogowe lub inną dokumentację techniczną z zaznaczeniem na nich wyspecyfikowanych parametrów.

W okresie gwarancji Zamawiający wymaga wsparcia Wykonawcy w zakresie obsługi sprzętu i oprogramowania będącego przedmiotem Umowy oraz aktualizacji oprogramowania w łącznej ilości 50 godzin.

Wykonawca jest zobowiązany dostarczyć Dokumentację powykonawczą, która musi być sporządzona zgodnie z poniższym szablonem, przy czym szablon może zostać uzupełniony o dodatkowe elementy przez Wykonawcę:

1. Opis wdrożonych systemów i aplikacji.
 - a. Opis systemu.
 - b. Funkcjonalności
 - c. Zależność pomiędzy wszystkimi elementami Rozwiązania.
2. Opis przepływu danych pomiędzy poszczególnymi Modułami wraz ze schematami graficznymi.
3. Sposób instalacji i konfiguracji Rozwiązania:
4. Wymagane licencje - wykaz niezbędnych licencji.

Nr referencyjny: RSID.271.39.2025

Zadanie 1.

Zakup i wdrożenie serwera wraz z oprogramowaniem

Zamawiający informuje, że posiada 2 serwery HPE DL385 G10 V2 pracujące w klastrze wirtualizacyjnym VMware HA oparte o procesory AMD EPYC 7313

Ze względów gwarancyjnych oraz kompatybilności i wymienności komponentów Zamawiający wymaga dostawy 1 szt takiego samego serwera o parametrach minimalnych opisanych poniżej:

Dopuszcza się zaoferowanie innej konfiguracji serwera wyłącznie pod warunkiem, że Wykonawca dostarczy kompletną platformę wirtualizacyjną składającą się z co najmniej 3 (trzech) serwerów fizycznych o jednolitej architekturze procesorowej, tworzących odrębny, spójny klaster wirtualizacyjny z pełną obsługą mechanizmów wysokiej dostępności i migracji maszyn wirtualnych w obrębie tej platformy.

Za spełnienie warunku dostawy 1 szt takiego samego serwera uznaje się dostawę serwera z tej samej linii produktowej producenta oraz tego samego typu procesora umożliwiającego zastosowanie technologii VMware vMotion / Hyper-V Live Migration

Ciężar wykazania równoważności technicznej i funkcjonalnej zaoferowanej platformy wirtualizacyjnej spoczywa na Wykonawcy.

W przypadku zastosowania rozwiązania równoważnego, cały proces migracji i konfiguracji nowych serwerów do istniejącego klastra wirtualizacyjnego leży po stronie oferenta. Migrację należy przeprowadzić w taki sposób, aby nie zakłócać ciągłości pracy Urzędu oraz nie utracić żadnych danych.

Zamawiający posiada licencje oprogramowania VMware konieczne do dołączenia do platformy w/w serwera.

Parametry techniczne serwera – należy dostarczyć 1 sztukę

L.p.	Cecha	Wymagania minimalne
1.	Obudowa	Maksymalnie 2U RACK 19 cali (wraz z szynami montażowymi oraz ramieniem do prowadzenia kabli, umożliwiającymi serwisowanie serwera w szafie rack bez jego wyłączenia).
2.	Procesory	2 procesory o parametrach opisanych poniżej.

Nr referencyjny: RSID.271.39.2025

		<p>Procesor min. 16 rdzeniowy, x86 - 64 bity, osiągający w testach SPECrate2017_int_base wynik minimum 300 punktów dla oferowanego modelu serwera, wyposażonego w dwa procesory. Wyniki testu muszą być dostępne na stronie www.spec.org.</p> <p>Procesor taktowany częstotliwością min. 3.0 GHz. Serwer umożliwiający obsługę procesorów 64 rdzeniowych.</p>
3.	Pamięć operacyjna	Zainstalowane 512 GB pamięci RAM typu DDR4 Registered, 3200MT/s w kościach o pojemności 32 GB. Obsługa zabezpieczeń: Advanced ECC.
4.	Sloty rozszerzeń	<p>Serwer musi posiadać minimum 2 aktywne gniazda PCI-Express generacji 4, Full-height (pełnej wysokości) i full-length (pełnej długości) oraz 1 aktywne gniazda PCI-Express generacji 4, Full-height (pełnej wysokości) i half-length (połowy długości), gotowe do obsadzenia kartami rozszerzeń (z dostępem zewnętrznym), w tym min. 1 sloty x16 (szybkość slotu – bus width) i 2 sloty x8 (szybkość slotu – bus width).</p> <p>Możliwość zainstalowania w serwerze 8 slotów PCI-Express generacji 4, Full-height (pełnej wysokości) i full-length (pełnej długości). Wymagany dodatkowy slot LOM lub OCP do obsługi kart Ethernet 10Gb/25Gb.</p>
5.	Dysk twardy	<p>Wolne zatoki dyskowe gotowe do zainstalowania 8 dysków typu Hot Swap, SAS/SATA/SSD, 3,5"</p> <p>Zainstalowane 2 dyski SSD o pojemności 480GB skonfigurowane w RAID-1 ze wsparciem dla oprogramowania VMware.</p>
6.	Interfejsy sieciowe	<p>Serwer musi być wyposażony w:</p> <ul style="list-style-type: none"> - 4 porty 10/25 SFP28 <p>Oferowane karty do połączeń LAN (2 porty) muszą znajdować się na liście kart certyfikowanych z ESXi 7 lub nowszym.</p> <p>Oferowane karty do połączeń SAN (2 porty) muszą obsługiwać operacje bezstratne (tzw. Lossless Networking).</p> <p>Wraz z serwerem należy dostarczyć 2 szt. oryginalnych kabli producenta SFP28 25 GbE.</p> <p>Długość kabli 3-5m.</p> <p>Wraz z serwerem należy dostarczyć 2 szt. oryginalnych modułów producenta SFP+ 10 GbE na odległość do 30m (MM).</p>
7.	Karta graficzna	Zintegrowana karta graficzna
8.	Porty	<p>4 porty USB min. 3.0 w tym 2 wewnętrzne</p> <p>Port VGA</p> <p>Możliwość doposażania serwera w port szeregowy typu DB9/DE-9 (9 pinowy) wyprowadzony na zewnątrz obudowy bez pośrednictwa portu USB/RJ45.</p> <p>Ilość dostępnych złącz VGA i USB nie może być osiągnięta poprzez stosowanie zewnętrznych przejściówek, rozgałęziaczy czy dodatkowych kart rozszerzeń zajmujących jakikolwiek slot PCI Express serwera..</p>

Nr referencyjny: RSID.271.39.2025

9.	Zasilacz	2 szt., typu Hot-plug, redundantne, każdy o mocy minimum 800W.
10.	Chłodzenie	Zestaw wentylatorów redundantnych typu hot-plug
11.	Karta/moduł zarządzający i system zarządzania	<p>Niezależna od systemu operacyjnego, zintegrowana z płytą główną serwera lub jako dodatkowa karta w slotcie PCI Express, jednak nie może ona powodować zmniejszenia minimalnej wymaganej liczby gniazd PCIe w serwerze, posiadająca minimalną funkcjonalność:</p> <ul style="list-style-type: none"> • monitorowanie podzespołów serwera: temperatura, zasilacze, wentylatory, procesory, pamięć RAM, kontrolery macierzowe i dyski (fizyczne i logiczne), karty sieciowe • możliwość pracy w trybie bezagentowym – bez agentów zarządzania instalowanych w systemie operacyjnym z generowaniem alertów SNMP • dostęp do karty zarządzającej poprzez <ul style="list-style-type: none"> - dedykowany port RJ45 z tyłu serwera lub - przez współdzielony port zintegrowanej karty sieciowej serwera; • dostęp do karty możliwy <ul style="list-style-type: none"> - z poziomu przeglądarki webowej (GUI); - z poziomu linii komend; • wirtualna zdalna konsola, tekstowa i graficzna, z dostępem do myszy i klawiatury i możliwością podłączenia wirtualnych napędów CD/DVD i USB i wirtualnych folderów; • monitorowanie zasilania oraz zużycia energii przez serwer w czasie rzeczywistym z możliwością graficznej prezentacji; • konfiguracja maksymalnego poziomu pobieranej mocy przez serwer (capping); • zdalna aktualizacja oprogramowania (firmware); • wsparcie dla Microsoft Active Directory; • wsparcie dla IPv4 oraz IPv6, obsługa SNMP v3 oraz RESTful API; • możliwość autokonfiguracji sieci karty zarządzającej (DNS/DHCP);
12.	Wsparcie dla systemów operacyjnych	<p>VMware vSphere 7.0. U2/U3</p> <p>Microsoft Windows Server 2019 i 2022</p> <p>Red Hat Enterprise Linux (RHEL)</p> <p>SUSE Linux Enterprise Server 15 SP1</p>
13.	Inne	<p>Płyta główna musi być zaprojektowana przez producenta serwera.</p> <p>Serwer musi być fabrycznie nowy, wyprodukowany nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z oficjalnego kanału dystrybucyjnego producenta na rynek polski. Zamawiający zastrzega sobie, aby Wykonawca na żądanie Zamawiającego przedłożył</p>



Fundusze
Europejskie
Polska Cyfrowa



Rzeczpospolita
Polska

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Nr referencyjny: RSID.271.39.2025

		oświadczenie Producenta oferowanego sprzętu, w języku polskim, potwierdzające pochodzenie sprzętu z autoryzowanego kanału sprzedaży z Polski. Wymagany moduł TPM 2.0
14.	Wsparcie techniczne	Minimalnie 36 miesięczna gwarancja producenta w miejscu instalacji. 2-godzinny czas reakcji w godzinach od 9:00 do 17:00 (standardowe dni robocze)
15.	Oprogramowanie	Zamawiający wymaga dostarczenia licencji na Windows Serwer Datacenter 2022 w ilości zapewniającej pokrycie na oferowaną sumaryczną liczbę rdzeni we wszystkich oferowanych serwerach lub równoważne, tj. obsługujące technologię COM, .NET posiadające możliwości zarządzania komputerami oraz użytkownikami na poziomie funkcjonalności usługi katalogowej Active Directory opartej na Windows Serwer* i w pełni wspierające MS Exchange*, MS System Center Configuration Manager*, MS Lync* oraz umożliwiające implementację nieograniczonej licencyjnie liczby maszyn wirtualnych opartych o usługę Hyper-V .

Nr referencyjny: RSID.271.39.2025

Zadanie 2

Zakup i wdrożenie deduplikatora macierzy oraz upgrade istniejącego oprogramowania do backupu w celu obsługi deduplikacji

Zamawiający wymaga dostarczenia urządzenia typu deduplikator danych klasy enterprise (appliance do backupu z deduplikacją). Urządzenie musi realizować deduplikację danych na poziomie bloków lub segmentów, w trybie inline, we współpracy z oprogramowaniem do backupu, zapewniając istotne zmniejszenie ilości przechowywanych danych, możliwość replikacji z deduplikacją pomiędzy lokalizacjami oraz mechanizmy integralności i ochrony danych (kontrola spójności, ochrona przed przypadkowym lub nieautoryzowanym skasowaniem)..

Lp.	Opis funkcjonalny
1.	<p>Urządzenie ma oferować Moduł Integracyjny (MI) z oprogramowaniem NetBackup, Backup Exec, Data Protector, Veeam, Nakivo, Oracle RMAN, MS SQL oraz SAP HANA poprzez API realizujące funkcje:</p> <ul style="list-style-type: none"> a) Wykonania kopii zapasowej z zastosowaniem deduplikacji na źródle, serwerze backupu lub urządzeniu backupowym przez dowolnie wybrane medium transmisyjne WAN, LAN i SAN b) Samodzielnej syntezy pełnych kopii zapasowych bez transferu danych na urządzenia/serwery zewnętrzne. c) Zarządzania operacjami replikacji (wyłącznie unikalnych bloków - bez rehydracji) realizowaną bezpośrednio pomiędzy urządzeniami deduplikującymi przez sieć WAN/LAN d) Zarządzanie retencją danych e) Zarządzać migracją zdeduplikowanych i skompresowanych danych do chmurowej pamięci obiektowej protokołami AWS S3 i Azure Blob. f) MI musi być wspierany na platformach AIX, HP-UX, Windows, Linux w sieciach IP (IP4 oraz IP6) oraz SAN (FC).
2.	<p>Oferuje deduplikację zmiennym blokiem o średniej wielkości 4KB z funkcją sliding window w trybie in-line (w pamięci) urządzenia (współczynnik równoważności $W_1=0$) lub w konfiguracji równoważnej to jest:</p> <ul style="list-style-type: none"> a) dla urządzeń deduplikujących zmiennym blokiem o średniej wielkości do 8kB lub bez użycia sliding window należy zastosować współczynnik równoważności $W_1=0,5$ dla wymaganej specyfikacją pojemności netto i wydajności. b) dla urządzeń, dla których zalecane jest stosowanie jest bloku o stałej długości z przedziału 8-256kB współczynnik równoważności $W_1=1$ dla wymaganej specyfikacją pojemności netto i wydajności. c) urządzenia deduplikujące w trybie innym niż inline powinny być dostarczone z pamięcią podręczną zbudowaną z dysków SSD o pojemności netto równej dziennemu zrzutowi wyszczególnionym w specyfikacji
3.	Urządzenie musi posiadać na swej liście wsparcia i znajdować się na listach wsparcia bieżących wersji oprogramowania backupowego: NetBackup i Backup Exec, CommVault Simpana, IBM TSM, Data Protector, EMC Networker oraz oświadczenie producenta, że nie ogłosił rezygnacji ze wsparcia linii produktowych wyspecyfikowanych powyżej.
4.	Zapewnia replikację zdeduplikowanych zasobów poprzez sieć WAN/LAN (bez tzw. rehydracji) zarządzaną bezpośrednio przez oprogramowanie kopii zapasowych przez interfejsy OST lub dedykowane MI.
5.	<p>Oferowane urządzenie pozwala na równoczesny dostęp protokołami FC i iSCSI, NFS, CIFS przez zainstalowane w urządzeniu porty w ilości rekomendowanej przez producenta nie mniejszej niż:</p> <ul style="list-style-type: none"> a) 2x Ethernet 10 Gb Base-T (wspierające: LACP, Adaptive Load Balancing, VLAN) b) 2x10/25GbE z wkładkami 10Gb SR.
6.	Urządzenie zabezpiecza dane przechowywane lokalnie w technologii RAID6 oraz globalnie przez replikację/kopiowanie unikalnych i skompresowanych bloków danych wskazanych zasobów przez WAN
7.	Każda grupa RAID6 o ilości dysków w grupie większej niż 6 i/lub pojemności powyżej 4TB, musi posiadać dysk „hot spare” w ilości rekomendowanej przez producenta, nie mniejszej niż 6% ogólnej ilości dysków.
8.	<p>Urządzenie musi zawierać wszystkie niezbędne licencje dla dostarczonej pojemności do realizacji następujących funkcji:</p> <ul style="list-style-type: none"> a) Deduplikacji inline, b) dostęp po NFS, CIFS

Nr referencyjny: RSID.271.39.2025

Lp.	Opis funkcjonalny
	<ul style="list-style-type: none"> c) dostęp przez VTL d) dostęp przez Moduł Integracyjny e) centralny system zarządzania przez CLI i GUI dla zaoferowanych urządzeń f) centralny monitoring urządzeń g) licencję replikacji (bez rehydracji) z/do urządzenia z wykorzystaniem MI
9.	<p>Urządzenie musi oferować opcje bezpieczeństwa, tj.</p> <ul style="list-style-type: none"> a) szyfrowanie danych zgodnym z FIPS 140-2 CAVP/CMVP. Opcja szyfrowania powinna wybiórczo pozwalać na: <ul style="list-style-type: none"> o szyfrowanie transmisji danych po IP o szyfrowanie przechowywanych danych na każdym wskazanym zasobie urządzenia niezależnymi kluczami b) bezpiecznego kasowania wybranych obiektów z zasobów dyskowych zgodnie z NIST SP 800-88 c) Współpracować z centralnym zarządzaniem kluczami szyfrującymi zgodnym z KMIP, FIPS 140-2 Level 2 w szczególności z urządzeniami HPE ESKM oraz SafeNet KeySecure Appliance d) Dostarczona funkcjonalność i licencja replikacji przechowywanych na urządzeniu danych powinny zapewniać pełną kontrolę przez GUI, lub CLI nad szyfrowanymi zasobami, w tym na zmianę pojemności przeznaczonych na szyfrowane dane zasobów w zakresie od 1TB do pełnej zamówionej pojemności w dowolnym czasie użytkowania. <p>Funkcje muszą zapewniać niezależne i wybiórcze stosowanie dla wskazanych zasobów. Zarządzanie kluczami (1 per udział) ma zapewniać możliwości kopiowania i odtwarzania kluczy. (współczynnik równoważności $W_2=0$)</p>
10.	<p>W przypadku, jeśli urządzenie nie umożliwia selektywnej aktywacji szyfrowania opisanej powyżej oraz bezpiecznego kasowania na poziomie udostępnianego zasobu, Zamawiający zezwala na dostarczenie rozwiązania równoważnego spełniającego jedno z wymagań poniżej :</p> <ul style="list-style-type: none"> a) dostarczyć dodatkowe urządzenie o parametrach nie mniejszej niż wyspecyfikowana w zamówieniu przeznaczone na dane szyfrowane b) Dostarczyć urządzenie o wydajność uwzględniającej współczynnik równoważności $W_2=0,5$ dla wydajności wyspecyfikowanej w SIWZ.
11.	<p>Wsparcie dla funkcji automatycznego awaryjnego restartu wykonywanych zadań tworzenia/przywracania kopii zapasowych w ramach klastra kontrolerów. Zamawiający dopuszcza dostarczenie rozwiązania równoważnego t. j.:</p> <ul style="list-style-type: none"> e) dodatkowego urządzenia deduplikacyjne o parametrach nie mniejszych niż wyspecyfikowane w zamówieniu dla każdego ośrodka przetwarzania f) dedykowanych serwerów mediów w liczbie zapewniającej wykonywanie kopii zapasowych z wydajnością dwukrotnie wyższą od wyspecyfikowanej w zamówieniu skonfigurowanych tak, aby wykonywać kopie zapasowe na 2 lokalne urządzenia deduplikujące równolegle.
12.	Urządzenie umożliwia zarządzanie pasmem backupu, replikacji/kopiowania danych pomiędzy urządzeniami.
13.	<p>Dostarczenie na potrzeby Q/A i testów urządzenia o pojemności min. 1 TB.</p> <p>Zamawiający dopuszcza, urządzenia w postaci maszyny wirtualnej (o maksymalnych wymaganiach 2vCPU, 30GB RAM) na platformie ESXi, Hyper-V pod warunkiem, że producent udziela wsparcia dla stosowania go w środowiskach produkcyjnych.</p>
14.	Rozwiązanie powinno oferować centralną konsolę zarządzania pozwalającą na zarządzanie do 20 urządzeniami deduplikacyjnymi z jednej konsoli w zakresie raportowania (zajętości dysków, poziomów deduplikacji, replikacji danych, trendów) powiadamiania itp. z możliwością wyświetlania wykresów eksportu.
15.	<p>Urządzenie musi zapewnić możliwość bezpośredniej integracji z macierzami dyskowymi (np. 3PAR, Nimble) i środowiskiem VMWare. Integracja musi wykorzystywać snapshoty macierzowe do wykonywania konsystentnych kopii zapasowych (VADP) aplikacji bezpośrednio z macierzy na urządzenie StoreOnce. Integracja zapewnia przesyłanie wyłącznie unikalnych bloków snapshotów oraz syntezę pełnych kopii zapasowych na urządzeniu backupowym, w trybie inline bez udziału oprogramowania backupowego. Procesy tworzenia i przywracania kopii zapasowych mają być zintegrowane z konsolą vCenter oraz standardowym klientem VMware w zakresie retencji, tworzenia i przywracania kopii zapasowych i harmonogramów. Rozwiązanie musi oferować REST API umożliwiające integrację aplikacji ze snapshotami oraz oferowanym systemem backupowym w zakresie, co najmniej, raportowania.</p> <p>W przypadku braku opisanej integracji z macierzami produkcyjnymi należy zapewnić niezbędne licencje oprogramowania backupowego wspierające sprzętowe migawki na systemy objęte backupem w wymiarze 0,8 pojemności zamawianego urządzenia deduplikacyjnego.</p>
16.	W przypadku, jeśli producent nie specyfikuje na ogólnodostępnych stronach internetowych informacji dot. wydajności

Nr referencyjny: RSID.271.39.2025

Lp.	Opis funkcjonalny
	odtworzenia danych oferowanego urządzenia należy przyjąć, że wydajność odtworzenia wynosi 35% wydajności tworzenia kopii zapasowych przy zastosowaniu wskazanego przez dostawcę interfejsu tworzenia kopii zapasowych.
17.	Redundantne zasilanie (n+1)
18.	Proces usuwania przeterminowanych danych tzw. „housekeeping” musi działać w sposób ciągły, z zastrzeżeniem, że możliwe jest jego wstrzymanie w celu maksymalizacji wydajności procesów tworzenia/przywracania kopii zapasowych, lub dostarczone urządzenie dostarczone jest w konfiguracji równoważnej to jest zastosowano współczynnik równoważności $W_3=0,3$ dla wymaganej specyfikacją pojemności netto i wydajności. Rozwiązania o zalecanej częstotliwości uruchamiania procesów housekeeping mniejszej niż 12 godzin powinny być wyposażone w dodatkową pojemność dyskową – 30% wyspecyfikowanej w SIWZ.
19.	Wymogi serwisowe: <ul style="list-style-type: none"> • Objęcie wszystkich komponentów urządzenia polisą serwisową producenta przez 3 lata • Przyjęcie zgłoszeń w trybie 9x5, • Realizacja usług serwisowych w miejscu instalacji sprzętu • Uszkodzone dyski pozostają u Zamawiającego
20.	Oferowane urządzenie pochodzi z autoryzowanego kanału dystrybucji producenta w Polsce i jest objęte polskojęzycznym wsparciem w miejscu instalacji. Pisemne oświadczenia wystawione przez producenta podpisane i wystawione nie później niż w dniu podpisania umowy dotyczące zapewnienia: <ul style="list-style-type: none"> • gwarancji świadczonej w miejscu instalacji urządzenia z czasem reakcji następnego dnia roboczego (9x5) • oświadczenie, że dostarczone urządzenie będzie fabrycznie nowe, wyprodukowane w 2025 r. i pochodzi z autoryzowanego kanału producenta na terenie Polski • oświadczenie, że oferowane urządzenie jest zgodne ze wszystkimi zapisami specyfikacji technicznej przetargu
21.	Urządzenie w celu zapewnienia niezbędnych parametrów RTO, RPO, BW oraz wymagań retencji danych musi zapewniać: <ol style="list-style-type: none"> a) wydajność tworzenia kopii zapasowych równą iloczynowi $(1 + W_2 + W_3) * 25TB/h$ b) obsługę co najmniej 256 strumieni kopii zapasowych c) obsługę co najmniej 64 strumieni odtworzenia d) wydajności odtworzenia: 6TB/h e) pojemność netto po odjęciu narzutu RAID: $(1 + W_1 + W_3) * 128 TB$ udokumentowane w ogólnodostępnej na stronach producenta dokumentacji.
22.	Urządzenie ma być dostarczone w konfiguracji niezbędnej do osiągnięcia nominalnej wydajności oraz pojemności. W szczególności maksymalną wspieraną ilość RAM oraz innych elementów pomocniczych w szczególności dysków SSD/kart Flash zapewniających rozbudowę do nominalnej pojemności wyspecyfikowanej w karcie produktu.
23.	W ramach wsparcia należy dostarczyć chmurową usługę realizującą nst. zadania: <ol style="list-style-type: none"> a) Prezentującą historię i trendy wykorzystania urządzenia, b) analizę konfiguracji, wersji FW, Driverów LAN/SAN, konfiguracji i uaktualnienia OS, MI, driverów i FW kart HBA/NIC . c) Wykorzystania i poziomu deduplikacji danych o długiej retencji przesłanych przez urządzenie do chmury
24.	W celu optymalizacji wykorzystania urządzenie powinno umożliwiać dla zasobów o długiej retencji: <ol style="list-style-type: none"> a) wyniesione do chmury prywatnej/publicznej kompatybilnej z AZURE Blob, AWS S3 za pomocą wspieranej technologii MI. <ol style="list-style-type: none"> i. w formie skompresowanej i zdeduplikowanej algorytmem dostarczonego urządzenia w celu minimalizacji transferu danych ii. Transfer danych musi zachodzić wielowątkowo dla zapisu oraz odczytu danych z chmury. iii. Wyniesienie ma być wspierane w ramach integracji MI dla każdego wspieranego oprogramowania backup (ochrony danych). iv. Metadane dla przechowywanych w chmurze danych muszą być buforowane w urządzeniu dla szybkiego dostępu i minimalizacji transferu z chmury. v. Urządzenie powinno umożliwiać przechowywanie w chmurze danych o pojemności wymaganej w SIWZ dla urządzenia deduplikacyjnego.

Nr referencyjny: RSID.271.39.2025

Lp.	Opis funkcjonalny
	vi. Dane przechowywane w chmurze muszą być dostępne z dowolnego urządzenia deduplikacyjnego wspierającego pojemność wymaganą SIWZ'em dla celów DR. Dane przechowywane w chmurze muszą być przechowywane w formacie/trybie samo-opisującym umożliwiającym wykorzystanie także w przypadku utraty urządzenia deduplikacyjnego, które umieściło je w chmurze.
25.	Urządzenie musi posiadać możliwość zapewnienia niezmienności zapisanych danych przez określony czas. W zdefiniowanym okresie niezmienności Obiekty nie mogą być skasowane przez administratora, użytkownika lub oprogramowanie backup.

Oprogramowanie do backup-u

Zamawiający informuje, że jest w posiadaniu oprogramowania NAKIVO Backup & Replication Enterprise Essentials for VMware, Hyper-V, and Nutanix dla 6 procesorów.

Zamawiający wymaga podniesienia aktualnej wersji oprogramowania do nowej wersji wraz z równoczesnym zakupieniem 2 nowych licencji dla 2 dodatkowych procesorów o następujących minimalnych parametrach ze wsparciem producenta na okres do 2028-06-25.

Jako rozwiązanie równoważne Zamawiający uzna dostawę łącznie 8 (ośmiu) licencji, z których każda spełniała będzie niżej wymienione wymagania minimalne.

W przypadku zastosowania rozwiązania równoważnego, cały proces migracji i przeniesienia danych z posiadanego rozwiązania backupowego do nowego rozwiązania leży po stronie oferenta. Migrację należy przeprowadzić w taki sposób, aby nie zakłócać ciągłości pracy Urzędu oraz nie utracić żadnych danych.

	Nazwa
I	Wymagania minimalne
1	rozwiązanie musi zapewniać wsparcie backupu dla następujących platform wirtualizacyjnych, środowisk chmurowych i maszyn fizycznych przy czym obsługa poszczególnych z nich może być uwarunkowana wybranym typem licencji
a	Microsoft Server z rolą Hyper-V min. w wersjach 2025, 2022, 2019, 2016, 2012R2, 2012
b	Vmware vSphere min. w wersjach v5.5 - v8.0U2,
c	Nutanix AHV v6.5.4 (LTS)
d	Maszyny fizyczne: Windows Server 2025, 2022, 2019, 2016, 2012R2, 2012
e	Bazy danych Oracle (oprogramowanie powinno posiadać interfejs do komunikacji z agentem RMAN umożliwiającym backup baz danych Oracle zainstalowanych na systemie operacyjnym Windows Server)
2	Oprogramowanie musi wspierać wszystkie systemy operacyjne gościa, które są obsługiwane przez natywny backup środowisk VMware vSphere, MS Hyper-V
3	Oprogramowanie musi pozwalać na wdrożenie w środowiskach
a	na serwerze sprzętowym Windows lub Linux
b	jako maszyna wirtualna Vmware
c	jako maszyna wirtualna Amazon
d	na serwerze NAS: ASUSTOR, NETGEAR, QNAP, Synology i Western Digital
4	Oprogramowanie do backupu musi pozwalać na wykorzystanie dowolnego serwera oraz przestrzeni dyskowej (nie dedykowanych), za pośrednictwem protokołów CIFS lub NFS.
5	Oprogramowanie w celu backupu całych maszyn wirtualnych nie może wymagać instalacji agenta wewnątrz maszyny wirtualnej



Fundusze Europejskie
Polska Cyfrowa



Rzeczpospolita Polska

Unia Europejska
Europejski Fundusz Rozwoju Regionalnego



Nr referencyjny: RSID.271.39.2025

II	Licencjonowanie
	Wszystkie funkcje i komponenty oprogramowania dla środowisk Vmware i Hyper-V powinny być licencjonowane per gniazdo procesora w hostach wirtualizacyjnych służących za źródło backupu lub replikacji, przy czym backup baz danych Oracle z wykorzystaniem RMAN może wymagać dodatkowej licencji per baza danych. Licencjonowanie powinno być realizowane w wariantach wieczystym, w którym licencja nie ma terminu ważności.
1	
2	Oprogramowanie musi umożliwiać nieograniczoną rozbudowę licencji (ilości gniazd cpu) w obrębie środowiska
	W ramach dostarczonej licencji na określoną ilość gniazd procesorów wymagane jest zapewnienie 1 roku wsparcia technicznego producenta, zapewniającego dostęp do aktualizacji i poprawek oprogramowania oraz umożliwiającego kontakt z działem technicznym producenta w zakresie oferowanego oprogramowania
3	
	Licencjonowanie innych środowisk może być realizowane na zasadzie subskrypcji wymagającej zakupu dedykowanej licencji dla środowiska
4	
III	Ochrona danych
1	Oprogramowanie musi posiadać funkcje backupu i replikacji:
a	Backup maszyn wirtualnych Vmware
	Replikacja maszyn wirtualnych Vmware (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych).
b	Replikacja nie może wymagać utworzenia backupu
c	Backup maszyn wirtualnych Hyper-V
	Replikacja maszyn wirtualnych Hyper-V (tworzenie i aktualizacja identycznych kopii dla źródłowych maszyn wirtualnych).
d	Replikacja nie może wymagać utworzenia backupu
	Możliwość przesłania pierwszych kopii za pośrednictwem dysków zewnętrznych do lokalizacji docelowej oraz późniejsze wznowienie ochrony maszyn wirtualnych
e	
f	Możliwość określania pasma wykorzystywanego przez oprogramowanie do backupu globalnie lub per zadanie
g	Możliwość tworzenia do 1000 punktów przywracania dla każdej z maszyn wirtualnych w ramach zadania backupu
	Obsługa retencji zgodnie z zasadą Grandfather-father-son – oprogramowanie musi pozwalać na rotację punktów przywracania w trybie dziennym, tygodniowym, miesięcznym oraz rocznym
h	
	Kopia backupu (replikacja) do innych repozytoriów backupu lokalnych oraz zdalnych
	Oprogramowanie musi pozwalać na utworzenie kopii źródłowego repozytorium backupu oraz tylko wybranych backupów.
i	Kopia tworzona jest zgodnie z określonym harmonogramem
	Oprogramowanie musi pozwalać na określenie kolejności, w jakiej są backupowane lub replikowane maszyny wirtualne w ramach zadania
j	
	Oprogramowanie musi umożliwiać tworzenie scenariuszy odtwarzania w środowiskach wirtualnych składających się z wielu etapów np. wyłączenia/włączenia maszyny, odczekania określonego czasu, wykonania jednego lub wielu wcześniej utworzonych zadań backupu lub replikacji
k	
	Oprogramowanie musi udostępniać widok kalendarza z naniesionymi zadaniami backupu/replikacji w celu łatwiejszego zarządzania zadaniami w bardziej złożonych środowiskach
l	
	Backup bazy danych Oracle (oprogramowanie powinno posiadać interfejs do komunikacji z agentem RMAN umożliwiającym backup baz danych Oracle zainstalowanych na systemie operacyjnym Windows Server lub Linux)
m	
	Oprogramowanie musi umożliwiać integrację z zewnętrznymi magazynami danych minimum: EMC Data Domain, NEC
n	HYDRAsstor, HPE StoreOnce, HPE 3PAR, HPE Nimble
	Oprogramowanie musi umożliwiać backup maszyn wirtualnych Vmware z wykorzystaniem technologii migawek wykonywanych na poziomie magazynów danych HPE 3PAR oraz HPE Nimble.
o	
IV	Optymalizacja wykorzystania miejsca na dane
1	Oprogramowanie musi posiadać poniższe funkcje pozwalające na ograniczenie wielkości backupowanych danych:
	Deduplikacja backupu, która działa w ramach całego repozytorium backupu oraz obejmuje wszystkie dane, które są w tym repozytorium przechowywane
a	
b	Kompresja backupu, w tym konfigurowalny stopień kompresji
c	Automatyczne pomijanie plików i partycji wymiany w systemach Windows i Linux działających jako maszyny wirtualne
V	Spójność danych
1	Oprogramowanie musi posiadać poniższe funkcje, gwarantujące spójność danych:

Nr referencyjny: RSID.271.39.2025

a	Spójny backup i replikacja maszyn wirtualnych z systemami Windows i Linux
b	Oprogramowanie musi umożliwiać wykonywanie własnych skryptów przed wykonaniem backupu oraz po jego wykonaniu
c	Automatyczne usuwanie (trunking) logów transakcyjnych z poniższych aplikacji: Microsoft Exchange 2013 - 2019 Microsoft SQL 2012, 2014, 2016, 2017, 2019, 2022 Automatyczna weryfikacja utworzonych backupów oraz replik ze środowiska Vmware poprzez uruchamianie maszyny wirtualnej bezpośrednio z backupu lub uruchamianie repliki
d	Oprogramowanie pozwala na generowanie oraz automatyczne wysyłanie raportów ze zrzutami ekranu testowanych maszyn wirtualnych Vmware i Hyper-V
e	Pełna weryfikacja wszystkich danych przechowywanych w repozytorium backupu na żądanie, ze wskazaniem niespójnych punktów przywracania
f	Szyfrowanie danych przesyłanych przez sieć do zdalnego repozytorium backupu i/lub repozytorium replikacji
g	
VI	Przywracanie danych
1	Oprogramowanie musi posiadać poniższe funkcje:
a	Przywracanie pełnych maszyn wirtualnych z backupu do oryginalnego lub innego serwera wirtualizacji Uruchomienie maszyny wirtualnej bezpośrednio z plików backupu w środowisku VMware (bez wcześniejszego przywracania maszyny wirtualnej) oraz możliwość jej migracji do serwera produkcyjnego
b	Przywracanie pojedynczych plików czy folderów bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej)
c	Przywracanie pojedynczych obiektów z poniższych aplikacji, bezpośrednio z plików backupu (bez wcześniejszego przywracania całej maszyny wirtualnej z backupu czy rozpakowywania plików backupu): MS Exchange MS Active Directory MS SQL
d	
e	Migracja dysków maszyn wirtualnych pomiędzy środowiskami wirtualizacji Vmware i Hyper-V i odwrotnie.
f	Współpraca z zewnętrznymi serwerami skanującymi pod kątem malware.
g	
VII	Wydajność
1	Oprogramowanie do backupu musi pozwalać na:
a	Tworzenie backupu i replik przyrostowo przy wykorzystaniu VMware CBT oraz Hyper-V RCT
b	Wykonywanie backupów przyrostowych bez wymogu okresowego tworzenia kopii pełnych
c	Backup z pominięciem sieci lan dzięki opcjom dostępu bezpośredniego w sieciach SAN
d	Akcelerację sieciową umożliwiającą redukcję ilości danych przesyłanych w sieci
e	Wsparcie dla urządzeń oferujących dodatkową deduplikację danych
f	
g	
VIII	Zarządzanie
1	Oprogramowanie musi pozwalać na następujące formy zarządzania:
a	Być wyposażone w interfejs web do zarządzania wszystkimi aspektami związanymi z backupem i przywracaniem danych Umożliwiać wysyłanie powiadomień w formie email dotyczących wykonywanych zadań backupu, błędów, cyklicznych raportów oraz wiadomości email z załącznikami potwierdzającymi poprawność odtworzenia maszyn wirtualnych dla wybranych zadań w formie zrzutów ekranu z uruchomionej z backupu maszyny wirtualnej
b	Zadanie backupu musi mieć możliwość uruchamiania zgodnie z harmonogramem, z opcją dodawania wielu harmonogramów dla pojedynczego zadania
c	Pliki backupu muszą mieć możliwość eksportu z opcją wyboru rodzaju dysków do których będzie robiony eksport.
d	Oprogramowanie musi pozwalać na eksportowanie oraz importowanie konfiguracji na cele reinstalacji czy migracji
e	Oprogramowanie musi umożliwiać integrację z Active Directory
f	Oprogramowanie musi wspierać tzw. tryb multi tenant, umożliwiający podzielenie oprogramowania do backupu na kilka podinstancji zarządzanych z odrębnych interfejsów w celu rozłożenia zarządzania w złożonych środowiskach
g	

Nr referencyjny: RSID.271.39.2025

Zadanie 3

Zakup i wdrożenie oprogramowania do centralnego zarządzania i monitoringu urządzeń mobilnych.

Oprogramowanie systemu do zarządzania flotą urządzeń mobilnych dla min. 100 urządzeń musi spełniać co najmniej poniższe wymagania minimalne. Licencje wieczyste ze wsparciem na minimum 2 lata.

1. Wykonawca dostarczy i wdroży w infrastrukturze teleinformatycznej Zamawiającego, systemu do zarządzania flotą urządzeń mobilnych, zwanego dalej Systemem MDM (Mobile Device Management).
2. Wykonawca udzieli niewyłącznych licencji umożliwiających dołączenie ilości urządzeń mobilnych Zamawiającego, do konsoli Systemu MDM.
3. Wykonawca przeprowadzi szkolenia techniczne online dla Administratorów po stronie Zamawiającego w zakresie obsługi, konfiguracji oraz administracji Systemem MDM.

I. Wymagania dla architektury i serwera:

1. System musi umożliwiać instalację na maszynie wirtualnej lub fizycznej Zamawiającego.
2. System MDM musi posiadać dokumentację określającą wymagania maszyny wirtualnej lub fizycznej w zależności od ilości urządzeń do niej dołączonych.
3. Dokumentacja Systemu MDM musi zawierać wszystkie niezbędne informacje odnośnie wymagań sieciowych dla Systemu, w szczególności opis konfiguracji sieciowej opartej na ruchu przychodzącym/wychodzącym na poszczególnych portach.
4. System MDM nie może wymagać dodatkowych licencji dla baz danych.
5. System MDM nie może wymagać dodatkowych licencji dla systemów operacyjnych.
6. System MDM musi być kompatybilny z systemem operacyjnym posiadającym ważne wsparcie dla aktualizacji bezpieczeństwa przynajmniej w okresie dwóch najbliższych lat.
7. System MDM musi oferować wsparcie dla backupu maszyn wirtualnych (snapshot, checkpoint).
8. Konsola Systemu MDM musi być dostępna z poziomu przeglądarki.
9. Konsola Systemu MDM musi być dostępna w języku polskim.
10. Konsola Systemu MDM musi być dostępna w jasny i ciemny motyw kolorystyczny.
11. Konsola Systemu MDM musi oferować możliwość wymuszenia pojedynczej sesji logowania na koncie administratora.
12. Konsola Systemu MDM musi rejestrować udane i nieudane próby logowania na koncie administratora.
13. System MDM musi oferować obsługę zmiennych globalnych służących do parametryzacji i personalizacji konfiguracji zarządzanej kierowanej w urządzeń.
14. System MDM musi oferować obsługę zmiennych globalnych na poziomie użytkownika, urządzenia, kart SIM oraz certyfikatów.
15. System MDM musi oferować wbudowane centrum certyfikacji.
16. System MDM musi oferować wbudowany VPN.
17. System MDM musi oferować wsparcie dla protokołu SCEP.
18. System MDM musi oferować wsparcie dla Android Enterprise
19. System MDM musi oferować wsparcie dla Apple Business Manager (dawniej Apple DEP).
20. System MDM musi oferować wsparcie dla Apps and Books (dawniej Apple VPP).
21. System MDM musi oferować wsparcie dla Knox Mobile Enrollment.

Nr referencyjny: RSID.271.39.2025

22. System MDM musi oferować wsparcie dla Android zero-touch Enrollment.
23. System MDM musi oferować systemowe narzędzie do backupu serwera.
24. System MDM musi oferować wsparcie dla Active Directory.
25. System MDM musi oferować wsparcie dla LDAP.
26. System MDM musi ofertować automatyczny onboarding i offboarding użytkowników.
27. System MDM musi oferować wsparcie dla Azure Active Directory.
28. System MDM musi oferować logowanie jednokrotne (SSO) przy pomocy Azure Active Directory.
29. System MDM musi oferować automatyczną synchronizację użytkowników z usług katalogowych AD/LDAP/AAD.
30. System MDM musi oferować wsparcie dla Microsoft Exchange.
31. System MDM musi oferować wsparcie dla protokołów ActiveSync, POP, IMAP.
32. System MDM musi oferować mechanizm zabezpieczający dostęp do poczty elektronicznej weryfikowany na podstawie dotykowego składnika np. certyfikat użytkownika.
33. System MDM musi oferować dodawanie aplikacji z pliku (aplikacje typu in-house).
34. System MDM musi oferować import aplikacji ze sklepu z aplikacjami Google Play.
35. System MDM musi oferować import aplikacji ze sklepu z aplikacjami iTunes.
36. System MDM musi oferować dodawanie aplikacji z zewnętrznego zasobu.
37. System MDM musi oferować stosowanie konfiguracji zarządzanej dla aplikacji Android.
38. System MDM musi oferować stosowanie konfiguracji zarządzanej dla aplikacji iOS.
39. System MDM musi oferować stosowanie konfiguracji zarządzanej dla aplikacji typu in-house.
40. System MDM musi oferować konfiguracje ACL dla konsoli.
41. System MDM musi oferować możliwość zmiany motywów konsoli (główny kolor, logo, favicon).
42. System MDM musi oferować uwierzytelnianie dwuskładnikowe dla użytkowników konsoli.
43. System MDM musi oferować wbudowany audyt integralności danych i bezpieczeństwa serwera.
44. System MDM musi obsługiwać wysyłanie niestandardowych profili konfiguracyjnych do urządzeń iOS.
45. System MDM musi gromadzić logi audytowe aplikacji.
46. System MDM musi gromadzić logi sieciowe aplikacji.
47. System MDM musi oferować konfigurowalną lokalizację Google Play i App Store.
48. System MDM musi oferować możliwość włączenia dostępu do całej treści zarządzanego sklepu Google Play bez konieczności logowania oraz nałożenie białej lub czarnej listy aplikacji.
49. System MDM musi oferować możliwość przejęcia kontroli zdalnej nad urządzeniem.
50. System MDM musi umożliwiać wykorzystanie klawiatury komputera do wpisywania tekstu na urządzeniu, podczas przejmowania kontroli zdalnej nad urządzeniem.
51. System MDM musi oferować automatyczne i manualne aktualizacje serwera.
52. System MDM musi oferować możliwość aktywowania użytkownika serwisowego celem sesji zdalnej adresowanej dla działu wsparcia producenta.

II. Wspierane systemy urządzeń mobilnych

1. Android 8.0 i nowszy.
2. iOS 13 i nowszy.
3. Windows 10/11 Pro/Enterprise.
4. MacOS 11 i nowszy

Nr referencyjny: RSID.271.39.2025

III. Rejestracja urządzeń w Systemie MDM

1. Rejestracja za pomocą aplikacji poprzez podanie loginu i hasła lub skanu kodu QR.
2. Rejestracja za pomocą kodu QR.
3. Rejestracja za pomocą tagów NFC.
4. Automatyczne dodawanie urządzenia do systemu.
5. Automatyczne dodawanie urządzenia do systemu i powiązanie z przypisanym użytkownikiem.
6. Rejestracja bez użytkownika.
7. Rejestracja z wykorzystaniem Knox Mobile Enrollment.
8. Rejestracja z wykorzystaniem Apple Business Manager.
9. Rejestracja z wykorzystaniem Android zero-touch.
10. Rejestracja za pomocą kodów QR oraz tagów NFC musi ofertować możliwość zapisania danych sieci WiFi.

IV. Pobierane informacje o zarządzanym urządzeniu

1. Informacja o producencie.
2. Informacja o modelu.
3. Informacja o systemie operacyjnym.
4. Informacja o stanie baterii.
5. Informacja o pamięć wewnętrznej.
6. Informacja o pamięci RAM.
7. Informacja o procesorze.
8. Informacja o operatorze używanych kart SIM.
9. Informacja o język urządzenia.
10. Informacja o szyfrowanie danych na urządzeniu.
11. Informacja o IP sieci komórkowej.
12. Informacja o IP sieci Wi-Fi.
13. Informacja o adresie MAC sieci Wi-Fi.
14. Informacja o SSID podłączonej sieci Wi-Fi.
15. Informacja o ICCID używanych kart SIM.
16. Informacja o numerze telefonu.
17. Informacja o IMEI gniazd kart SIM.
18. Informacja o numerze seryjnym.
19. Informacja o ostatnim kontakcie urządzenia z serwerem.
20. Informacja o wykorzystaniu karty SD.
21. Informacja o dostępności aktualizacji systemu operacyjnego.
22. Informacja o aplikacjach na urządzeniu wraz z wersją aplikacji.
23. System MDM musi oferować możliwość wykonania raportu wykorzystania pamięci urządzenia.
24. System MDM musi oferować możliwość wykonania raportu wykorzystania danych mobilnych na urządzeniu.
25. System MDM musi oferować możliwość wykonania raportu wykorzystania danych przez Wi-Fi na urządzeniu.
26. System MDM musi oferować możliwość wykonania raportu wykorzystania aplikacji na urządzeniu.

V. Wspierane konfiguracje urządzeń

Nr referencyjny: RSID.271.39.2025

1. System MDM musi oferować możliwość blokady urządzenia.
2. System MDM musi oferować możliwość wykonania zdjęcia podczas blokady urządzenia.
3. System MDM musi oferować możliwość resetu hasła.
4. System MDM musi oferować możliwość zmiany hasła przez administratora.
5. System MDM musi oferować możliwość przywrócenia urządzeń do ustawień fabrycznych.
6. System MDM musi oferować możliwość usunięcia danych służbowych z urządzeń.
7. System MDM musi oferować możliwość zablokowania ekranu urządzenia.
8. System MDM musi oferować możliwość wysłania notyfikacji.
9. System MDM musi oferować możliwość wysłania alarmu wraz z potwierdzeniem jego otrzymania i przeczytania.
10. System MDM musi oferować możliwość przekierowania połączeń na dowolny podany numer telefonu.
11. System MDM musi oferować możliwość restartu urządzenia.
12. System MDM musi oferować możliwość eksportu SMS.
13. System MDM musi oferować możliwość eksportu kontaktów.
14. System MDM musi oferować możliwość eksportu dziennika połączeń.
15. System MDM musi oferować możliwość eksportu logów audytowych z urządzenia.
16. System MDM musi oferować możliwość lokalizacji urządzeń na żądanie.
17. System MDM musi oferować możliwość lokalizacji urządzeń w interwałach czasowych.
18. System MDM musi oferować możliwość lokalizacji urządzeń w ruchu.
19. System MDM musi oferować możliwość zbierania historii lokalizacji urządzeń.
20. System MDM musi oferować możliwość zastosowania ograniczeń czasowych dla zbierania lokalizacji urządzeń.
21. System MDM musi oferować możliwość filtrowania urządzeń po ich lokalizacji.
22. System MDM musi oferować możliwość zablokowania i odblokowania aplikacji na urządzeniu.
23. System MDM musi oferować możliwość uruchomienia aplikacji na urządzeniu.
24. System MDM musi oferować możliwość zarządzanej konfiguracji dla aplikacji ze sklepu Google Play oraz App Store.
25. System MDM musi oferować możliwość zarządzanej konfiguracji dla aplikacji z pliku.
26. System MDM musi oferować możliwość wysłania konfiguracji aplikacji na urządzenie.
27. System MDM musi oferować możliwość usunięcia aplikacji z urządzenia.
28. System MDM musi oferować możliwość backupu SMS i MMS.
29. System MDM musi oferować możliwość backupu kontaktów.
30. System MDM musi oferować możliwość backupu dziennika połączeń.
31. System MDM musi oferować możliwość wykonania kopii zapasowej urządzenia Android bez konieczności rejestracji urządzenia (samodzielny system kopii zapasowej).
32. System MDM musi oferować możliwość instalacji aplikacji ze sklepu oraz z pliku.
33. System MDM musi oferować możliwość cichej instalacji aplikacji.
34. System MDM musi oferować możliwość instalacji skonfigurowanych aplikacji.
35. System MDM musi oferować możliwość zarządzania uprawnieniami aplikacji.
36. System MDM musi oferować możliwość uruchomienia służbowego sklepu z aplikacjami.
37. System MDM musi oferować możliwość włączenia Activation Lock.
38. System MDM musi oferować możliwość wyłączenia Activation Lock.
39. System MDM musi oferować możliwość dostarczenia konfiguracji ActiveSync.

Nr referencyjny: RSID.271.39.2025

40. System MDM musi oferować możliwość konfiguracji ActiveSync z szyfrowaniem S/MIME.
41. System MDM musi oferować możliwość dostarczenia konfiguracji IMAP/POP.
42. System MDM musi oferować możliwość konfiguracji Wi-Fi.
43. System MDM musi oferować możliwość konfiguracji Enterprise Wi-Fi.
44. System MDM musi oferować możliwość konfiguracji SCEP.
45. System MDM musi oferować możliwość dostarczenia certyfikatu na urządzenie.
46. System MDM musi oferować możliwość konfiguracji VPN w tym VPN per aplikacja.
47. System MDM musi oferować możliwość stworzenia białej i czarnej listy aplikacji dla przestrzeni służbowej.
48. System MDM musi oferować możliwość stworzenia białej i czarnej listy aplikacji dla przestrzeni prywatnej.
49. System MDM musi oferować możliwość stworzenia białej lista aplikacji podczas przemieszczania się urządzenia.
50. System MDM musi oferować możliwość dostarczenia i zarządzania kontaktami służbowymi.
51. System MDM musi oferować możliwość dostarczenia dokumentów służbowych.
52. System MDM musi oferować możliwość pobierania udostępnionych plików automatycznie.
53. System MDM musi oferować możliwość konfiguracji tapety.
54. System MDM musi oferować możliwość dostarczenia konfiguracji APN.
55. System MDM musi oferować możliwość konfiguracji trybu kiosk – pojedyncza aplikacja i wiele aplikacji.
56. System MDM musi oferować możliwość konfiguracji trybu kiosk - wiele aplikacji z logowaniem użytkownika do urządzenia.
57. System MDM musi oferować możliwość konfiguracji aplikacji „OEM Config” w szczególności Knox Service Plugin.
58. System MDM musi oferować możliwość zarządzania aktualizacjami systemu operacyjnego Android.
59. System MDM musi oferować możliwość ustawienia wymagań minimalnych hasła urządzenia.
60. System MDM musi oferować możliwość ustawienia wymagań minimalnych hasła w przestrzeni służbowej.
61. System MDM musi oferować możliwość użycia biometrii do odblokowania urządzenia.
62. System MDM musi oferować możliwość użycia biometrii do odblokowania przestrzeni służbowej.
63. System MDM musi oferować możliwość wyświetlania wiadomości na zablokowanym ekranie.
64. System MDM musi oferować możliwość zablokowania Bluetooth.
65. System MDM musi oferować możliwość wykrywania i reagowania na Root.
66. System MDM musi oferować możliwość wykrywania i reagowania na włączone debugowanie przez USB.
67. System MDM musi oferować możliwość wykrywania i reagowania na brak zaszyfrowania urządzenia.
68. System MDM musi oferować możliwość wykrywania i reagowania na włączone opcje developerskie.
69. System MDM musi oferować możliwość wykrywania i reagowania na podatność BlueBorne.
70. System MDM musi oferować możliwość wykrywania i reagowania na wyłączony SELinux.
71. System MDM musi oferować możliwość wykrywania i reagowania na niezaufanych administratorów urządzenia.
72. System MDM musi oferować możliwość wykrywania i reagowania na instalacje niedozwolonej aplikacji.
73. System MDM musi oferować możliwość wykrywania i reagowania na połączenie do niezabezpieczonej sieci Wi-Fi.
74. System MDM musi oferować możliwość wykrywania i reagowania na zmianę konfiguracji DNS.
75. System MDM musi oferować możliwość wykrywania i reagowania na zmianę konfiguracji Proxy.
76. System MDM musi oferować możliwość wykrywania i reagowania na zmianę konfiguracji Gateway.
77. System MDM musi oferować możliwość zablokowania użycia danych mobilnych w roamingu.

Nr referencyjny: RSID.271.39.2025

78. System MDM musi oferować rejestrację urządzeń Android w usłudze Azure Active Directory.
79. System MDM musi oferować wsparcie obsługi dostępu warunkowego (Conditional Access) do zasobów Office365 dla urządzeń Android.
80. System MDM musi oferować możliwość zablokowania tetheringu i mobilnych hotspotów.
81. System MDM musi oferować możliwość zablokowania dodawania nowych konfiguracji Wi-Fi.
82. System MDM musi oferować możliwość zablokowania podłączania nośników fizycznych.
83. System MDM musi oferować możliwość zablokowania połączeń wychodzących.
84. System MDM musi oferować możliwość zablokowania SMS.
85. System MDM musi oferować możliwość zablokowania transferu plików przez USB.
86. System MDM musi oferować możliwość ustawiania metod wprowadzania danych.
87. System MDM musi oferować możliwość zarządzania usługami lokalizacji.
88. System MDM musi oferować możliwość określania sposobu nadawania uprawnień aplikacji.
89. System MDM musi oferować możliwość określania sposobu aktualizacji aplikacji ze sklepu Google Play.
90. System MDM musi oferować możliwość zablokowania dodawania użytkowników nowych użytkowników do urządzenia.
91. System MDM musi oferować możliwość zablokowania zrzutów ekranu.
92. System MDM musi oferować możliwość zablokowania opcji deweloperskich.
93. System MDM musi oferować możliwość zablokowania trybu awaryjnego.
94. System MDM musi oferować możliwość zablokowania przywracania urządzeń do ustawień fabrycznych przez użytkownika.
95. System MDM musi oferować możliwość zablokowania dodawania nowych kont Google.
96. System MDM musi oferować możliwość zablokowania instalowania aplikacji z nieznanego źródła.
97. System MDM musi oferować możliwość wymuszania cyklicznego połączenia urządzenia z serwerem.
98. System MDM musi oferować możliwość wykonania akcji w przypadku przekroczenia czasu nieaktywności.
99. System MDM musi oferować możliwość zablokowania Smart Lock.
100. System MDM musi oferować możliwość zablokowania OTG przez USB.
101. System MDM musi oferować możliwość zablokowania mikrofonu.
102. System MDM musi oferować możliwość zablokowania zmian tapety.
103. System MDM musi oferować możliwość SIM pinning (ochrona przed użyciem służbowej karty SIM w urządzeniu innym niż służbowe).
104. System MDM musi oferować możliwość zablokowania FaceTime.
105. System MDM musi oferować możliwość zablokowania zrzutów ekranu i nagrywania ekranu.
106. System MDM musi oferować możliwość zablokowania AirDrop.
107. System MDM musi oferować możliwość zablokowania iMessage.
108. System MDM musi oferować możliwość zablokowania usług Apple Music.
109. System MDM musi oferować możliwość zablokowania usługi radio.
110. Zablokowanie głosowego wybierania numeru na zablokowanym ekranie.
111. System MDM musi oferować możliwość zablokowania Siri.
112. System MDM musi oferować możliwość zablokowania iBooks.
113. System MDM musi oferować możliwość zablokowania zakupów w aplikacji.
114. System MDM musi oferować możliwość zablokowania hasła iTunes podczas zakupów.
115. System MDM musi oferować możliwość zablokowania iCloud backup.
116. System MDM musi oferować możliwość zablokowania synchronizacji dokumentów w iCloud.

Nr referencyjny: RSID.271.39.2025

- 117.System MDM musi oferować możliwość zablokowania Keychain w iCloud.
- 118.System MDM musi oferować możliwość zablokowania backupu iCloud aplikacjach zarządzanych.
- 119.System MDM musi oferować możliwość zablokowania backupu służbowych książek.
- 120.System MDM musi oferować możliwość zablokowania dzielenia zdjęć z iCloud.
- 121.System MDM musi oferować możliwość zablokowania biblioteki zdjęć z iCloud.
- 122.System MDM musi oferować możliwość zablokowania My Photo Stream.
- 123.System MDM musi oferować możliwość wymuszenia ograniczonego śledzenia reklam.
- 124.System MDM musi oferować możliwość zablokowania niezaufanych certyfikatów TLS.
- 125.System MDM musi oferować możliwość zablokowania instalacji profili konfiguracyjnych.
- 126.System MDM musi oferować możliwość zablokowania modyfikowania kont.
- 127.System MDM musi oferować możliwość zablokowania zmiany nazwy urządzenia.
- 128.System MDM musi oferować możliwość zablokowania Handoff.
- 129.System MDM musi oferować możliwość zablokowania wyników wyszukiwania z Internetu w Spotlight.
- 130.System MDM musi oferować możliwość zablokowania wysyłania danych diagnostycznych Apple.
- 131.System MDM musi oferować możliwość zablokowania wykrywania Apple Watch.
- 132.System MDM musi oferować możliwość zablokowania parowania Apple Watch.
- 133.System MDM musi oferować możliwość zablokowania klawiatury predykcyjnej.
- 134.System MDM musi oferować możliwość zablokowania skrótów klawiszowych.
- 135.System MDM musi oferować możliwość zablokowania autokorekty.
- 136.System MDM musi oferować możliwość zablokowania sprawdzania pisowni.
- 137.System MDM musi oferować możliwość zablokowania Control Center na ekranie blokady.
- 138.System MDM musi oferować możliwość zablokowania Notification Center na ekranie blokady.
- 139.System MDM musi oferować możliwość zablokowania widoku Today na ekranie blokady.
- 140.System MDM musi oferować możliwość zablokowania AirPrint.
- 141.System MDM musi oferować możliwość zablokowania przechowywania poświadczeń AirPrint.
- 142.System MDM musi oferować możliwość zablokowania wykrywania iBeacon w AirPrint.
- 143.System MDM musi oferować możliwość zablokowania dyktowania.
- 144.System MDM musi oferować możliwość zablokowania modyfikacji eSIM.
- 145.System MDM musi oferować możliwość zablokowania autouzupełniania haseł.
- 146.System MDM musi oferować możliwość zablokowania pytania o hasło z pobliskich urządzeń.
- 147.System MDM musi oferować możliwość opóźnienia aktualizacji systemu operacyjnego.
- 148.System MDM musi oferować możliwość wymuszenia korzystania z Wi-Fi.
- 149.System MDM musi oferować możliwość zablokowania iTunes.
- 150.System MDM musi oferować możliwość zablokowania News.
- 151.System MDM musi oferować możliwość zablokowania Podcasts.
- 152.System MDM musi oferować możliwość zablokowania Game Center.
- 153.System MDM musi oferować możliwość zablokowania Safari.
- 154.System MDM musi oferować możliwość konfiguracji Safari.
- 155.System MDM musi oferować możliwość zablokowania App Store.
- 156.System MDM musi oferować możliwość zablokowania klawiatury QuickPath.
- 157.System MDM musi oferować możliwość zablokowania dostępu Files do dysków sieciowych.
- 158.System MDM musi oferować możliwość zablokowania dostępu Files do dysków USB.
- 159.System MDM musi oferować możliwość zablokowania Find My Device.



**Fundusze
Europejskie**
Polska Cyfrowa



**Rzeczpospolita
Polska**

Unia Europejska
Europejski Fundusz
Rozwoju Regionalnego



Nr referencyjny: RSID.271.39.2025

160.System MDM musi oferować możliwość zablokowania Find My Friends.

161.System MDM musi oferować możliwość zablokowania usuwania aplikacji systemowych.

162.System MDM musi oferować możliwość filtrowania treści w Safari.